Security & Defence Agenda

Report

Defining cyber-security

9 November 2011

SDA CYBER-SECURITY INITIATIVE

More information at www.securitydefenceagenda.org

A *Security & Defence Agenda* Report
Rapporteur: Jonathan Dowdall
Photos: Philippe Molitor - Gleamlight

Publisher: Geert Cami
Date of publication: November 2011

SECURITY & DEFENCE AGENDA
Bibliothèque Solvay, Parc Léopold,
137 rue Belliard, B-1040, Brussels, Belgium
T: +32 (0)2 737 91 48 F: +32 (0)2 736 32 16

Programme

Evening debate – 9 November 2011

Stanhope Hotel, Brussels, 17:30-19:00

Cyber-security stakeholders, actors and victims span governments, national and international institutions, major corporations and interest groups. This debate opens a new SDA series that seeks to make sense of the confusion over cyber-security and cyber-crime, and examines the cooperation mechanisms both in place and urgently needed. How vulnerable is Europe to cyber-attack, and what EU-level measures are now under discussion? How does Europe compare in the global drive to promote cyber-protection? What concrete actions should now be taken at national and international level, and how can these actions be coordinated?

Keynote speech by

Cecilia Malmström, European Commissioner for Home Affairs

Speakers:

Robert G. Bell, Senior Civilian Representative of the Secretary of Defense in Europe & Defense Advisor of the US Ambassador to NATO

Maj. Gen. Isaac Ben-Israel, Senior Cyber-Security Advisor to the Prime Minister, Israel

Maj. Gen. Patrick Fermier, Director, NATO HQ C3 Staff

Paul MacGregor, Director, Finmeccanica Cyber Solutions

Troels Oerting, Assistant Director for Operations, Europol

Florian Walther, Senior IT-Security Consultant, Curesec

Defining cyber-security

At the inaugural launch of the SDA's Cyber-security Initiative, a high-ranking panel and assembled experts gathered to discuss the core question of "defining cyber-security".

In her keynote address, European Commissioner for Home Affairs Cecilia Malmström cautioned that denial about the scale of threats in cyberspace is naïve. "This is a battle we may not win", she warned, with cyberspace being a domain in which "we need to act and need to protect as quickly as possible".

The Commissioner went on to outline three key initiatives being undertaken by the EU in this area. Firstly, a European cyber-crime centre will be set up by 2013. This will provide a central hub for all cyber-crime actions undertaken by national authorities, computer emergency response teams (CERTs) and Europol; as "without information sharing, there are very few concrete actions we can take".

"Without information sharing,
there are very few concrete actions we can take".

Secondly, the Commission will develop an overarching cyberspace strategy by 2012, to help establish the hierarchy and chain of information sharing between all relevant actors. In this field, "currently, some are working better then others, it is a work in progress", she explained.

Finally, the Commissioner affirmed that "we will not be able to do this unless we cooperate with other global partners", with NATO and the Council of Europe highlighted as being of particular importance. Above all, Malström called "on all governments and industry, to put this high on their agenda", and to partake in what is a "highly timely; highly relevant, discussion and exchange of views."

Senior Civilian Representative of the Secretary of Defense in Europe & Defense Advisor to the US Ambassador to NATO Robert Bell agreed that the scale of the threat goes far beyond typical defence and security policy. Citing recent high-level reports regarding the industrial espionage activity of Chinese and Russian hackers, Bell affirmed that "we have to be attuned to the economic dimensions of this – this could undercut our ability to enact policies… or even the economy and our ability to generate jobs."

Urgent action is clearly essential in the face of this challenge. Yet whilst NATO has a role to play, it is only "taking a lead, not *the* lead, on identifying standards that strike a balance between security on the one hand and affordability on the other."

Bell believes the future of cyber-security policy will be "an invitation for partnership. We are reaching out to countries around the world to build a consensus on the ideals of security, openness, transparency and innovation" in cyberspace. In this, "we have made progress", he affirmed.

Bell's final caution was about the creation of common standards. "It doesn't do us any good if the 28 member states at NATO recommend certain standards, when the 27 EU nations gathered down the road recommend another".

Next, Isaac Ben-Israel, Senior Cyber-Security Advisor to the Prime Minister of Israel, outlined a non-EU perspective. Ben-Israel explained how his government had prepared a list of 19 major infrastructures in need

of urgent protection in cyberspace, with power and water high on the list. However, "we faced a legal problem", he explained, "most of them were private sector infrastructures. We faced a dilemma: how do we encourage them to protect themselves from cyber-attacks?"

"We have a lot of attacks which are either criminal or hacking, but which are surely initiated by states – it is another form of warfare"

This private-public debate lies at the core of cyber-security, the he affirmed. "We found that it is a multidimensional problem, not a technological problem. There are legal, political and societal aspects – it is very complicated." Yet whilst complicated, it is also urgent. "We have a lot of attacks which are either criminal or hacking, but which are surely initiated by states – it is another form of warfare", he hinted.

From the military perspective, Maj. Gen. Patrick Fermier, Director of the NATO HQ C3 Staff, provided some insight to what NATO is doing in the cyber domain. The General urged participants to be cautious in the face of such a vast and challenging area. "Defining cyber-security is difficult – I'm not even sure we can do that right now, given the scope of the problem. I think we need to be humble in front of this threat."

He went on to explain how the North Atlantic Council had put the protection of NATO's critical systems high on the agenda, calling on them to "draw up an action plan for the policy implementation, and accelerating the already existing capability to protect NATO networks." For Fermier, the focus should be not just on preventing cyber-attacks, but also increasing resilience to their effects, as they will inevitably occur. "We need to be humble, and we need to develop this step by step", he concluded.

Paul MacGregor, Director of Finmeccanica Cyber Solutions, explained the technological challenges from an industry perspective. "We've all been seduced by the promises of cost efficiency and speed in cyberspace – that seduction has become an addiction, leaving us vulnerable to a new range of threats." Pointing out that cyber-attacks give an opponent the ability "to establish control over us using non-lethal power", MacGregor felt that the rise of information technology had made "everywhere a battlefield".

"There's a tendency to say that threats are now un-attributable, or that it is impossible to stop attacks – it isn't – in fact, 80% of vulnerabilities can be removed by simple technology, education and good practices."

Yet despite this widespread threat, the industry representative urged a level headed response. "There's a tendency to say that threats are now un-attributable, or that it is impossible to stop attacks – it isn't – in fact, 80% of vulnerabilities can be removed by simple technology, education and good practices." Once you have taken out this majority, "the remaining 20% is part of the bigger problem – ideological or state sponsored cyber-attacks", he explained. He was nonetheless confident a major leap forward in security could be facilitated by educating the public, and the purchase of basic cyber-security tools.

Defining cyber-security

Tackling the issue of cyber-crime, Troels Oerting, Assistant Director for Operations at Europol, confirmed that "the range of internet crime has reached huge levels – it now outpaces drug crime in scale." Whilst the range of tools at criminals' disposal has expanded to include more targeted and sophisticated methods, he did concede that not every act of cyber-crime carries the same significance. "Not everything in cyber-crime is big cyber-crime – there are 'Bicycle thefts' on the internet –it is our job to identify what are big attacks, and what are smaller threats."

However, getting this "big picture" will require more communication and awareness about cyber-crime. "We do not have all the resources we need yet" he lamented, "so we welcome the EU initiative for a cyber-crime centre", as discussed by the Commissioner. Such a centre should help Europol and other actors begin to "map" cyber-crime – to understand its networks and key players. "In this area we do not have the same knowledge as we do for conventional crime: we do not know if it is next door, or in Africa, or working by proxy". Yet Oerting was confident that "this will be solved."

Florian Walther, Senior IT-Security Consultant at Curesec, brought the debate round full circle to the question of defining cyber-security. Walther asked the provocative question to the panel: "Why do we see all this cyber-crime and attacks going up and up? We have had laws against cyber-crime and hacking for half a decade, but still, it continues." Why, he asked, is our basic cyber-security going down, even whilst we simultaneously give more attention to this policy area?

Cutting through the high level policy, the former hacker provided a simple answer. "Every threat and exploit is based on a vulnerability in our software", he explained. These vulnerabilities, propagated in cheap or poorly made software, "are the root cause" of our cyber-security problems. Walther thus put the fundamental questions of cyber-security at the door of the computer software industry. "If I sell a car and the brakes don't work, we have to recall that car – I am liable. But in IT, we can roll out software that is full of bugs and vulnerabilities – and it is the public that pays the price."

"If I sell a car and the brakes don't work, we have to recall that car – I am liable. But in IT, we can roll out software that is full of bugs and vulnerabilities – and it is the public that pays the price."

However, whilst many on the panel agreed this was a strong suggestion, Isaac Ben-Israel refuted the idea. "It sounds very convincing – the problem is all software; and all we need to do is legislate liability. But this is not really the problem," he countered. Using the car analogy, he pointed out that "car manufacturers only hold liability for malfunction, but not for damage caused by someone attacking a car." In Ben-Israel's opinion, the adversarial nature of cyber-security makes liability allocation irrelevant – a thinking opponent will seek out gaps in a system using all their ingenuity. "You cannot hold someone liable for this", he affirmed.

Walther responded the issue was not ingenuity of the attacker, but the gross ineptitude of the coding in software we expect to be secure. Referencing the infamous infection of nuclear centrifuges by the Stuxnet virus, he pointed out that these units had "lots and easy to exploit vulnerabilities" in their software.

Defining cyber-security

"Stuxnet would not have been possible without this", so software does have a fundamental responsibility.

These disagreements aside, the panel did agree with the overall assessment that "80%" of all vulnerabilities can be addressed through simple education of users, and the thorough application of basic cyber-security such as password protection. As Walther summarised, "we must shut down the first chunk" of basic cyber-security, so that "we will have more resources left over to tackle the really dangerous threats; the targeted threats and Government backed attacks which takes years to orchestrate, and could undermine the state."

Future Events

Public-private cooperation in cyber-security

EU-US cooperation in cyber-security

Cyber-protection of critical infrastructure